Amendments to the Specification

Please replace the paragraph at page 4 (page numbers are from the substitute specification), lines 6-15, with the following rewritten paragraph:

In systems that can be used for the sale of goods via networks such as the Internet, sales and delivery of goods can be conducted ~~to obtain~~ by obtaining order information through the network. The sales information can then be written to a database. In such a system, the data representing customer order information can be damaged during fraudulent acquisition of the data representing customer order information by hackers. In turn, ~~customers~~ customers' orders can be suspended and/or lost. Moreover, when customer order information is fraudulently stolen through the network, significant credit problems can occur for consumers. Conventionally, security systems known as firewalls are placed between the network and the internal system to reduce and/or prevent the likelihood of invasion by hackers.

Please replace the paragraph at page 4, lines 16-26, with the following rewritten paragraph:

Conventional firewall technology can require identification information, security codes and authentication to ensure access for those about to access the Internal system through the network. Such firewall technology is described, for example, in Japanese patent publications 11-298639, and ~~10-214304)~~ 10-214304. However, it [[-can]] can be difficult to protect against hackers who obtain identification information and security codes by fraudulent means and/or camouflage. To encourage general customers to place orders over the Internet, an ordering system is necessary that can reduce and/or prevent fraudulent data from becoming mixed with the data representing customer order information. Accordingly, a system is needed that can reduce and/or eliminate fraudulent reading of the contents of a database used in a system for sales of goods over a network.

Please replace the paragraph at page 5, lines 2-9, with the following rewritten paragraph:

An aspect of the present invention relates to a network security system ~~is provided~~ that includes a server connected to a network, a received data storage means to store data with an external format which a server received through the network, a received data format conversion means to convert data with an external format stored in the received data storage means to data with ~~the~~ an internal format and to store them in a received-process data storage means, and a host computer to execute a predetermined process utilizing data with the internal format stored in the received-process data storage means.

Please replace the paragraph at page 6, lines 1-16, with the following rewritten paragraph:

According to another aspect of the present invention, the received data storage means can allow data with an external format which the server received to be written, and can reduce the likelihood of and/or prevent data from being read out by the server. A received process data storage means can allow data with an internal format to be read out by the host computer and can reduce the likelihood of and/or prevent data from being written by the host computer. The received data storage means can reduce the likelihood of and/or prevent data from being read out by the server [[is]] by reducing the likelihood of and/or preventing the data in the received data storage means from being read out from the network side. Preventing the writing of data into the received process data means by the host computer can reduce the likelihood of and/or prevent data from being carelessly output from the host computer side to the network side. This can reduce the likelihood of and/or prevent data from flowing from the host computer to the network. Data on the host computer side is not read out to the network side. The likelihood of data being written or read out can be reduced and/or prevented. This includes all formats of data, whether internal or external.

Please replace the paragraph at page 16, lines 3-10, with the following rewritten paragraph:

In the example above, after the data with an external format 4 is converted to data with the internal format [[4]] 5 by the received data format conversion means 7, the storage process of this data with the internal format for addition to the database on the host computer side can be executed. However, these processes should be executed independently for the convenience of system operation. The conversion process by the received data format conversion means 7 is preferably executed when data with an external format is accumulated in some amount or when access to the server is not so busy.

Please replace the paragraph at page 16, lines 20-29, with the following rewritten paragraph:

The received data format conversion means 7 is not just an interface between the server and the host computer. The received data format conversion means 7 can also filter the one-way flow to extract and fabricate only the necessary data from data with an external format which might contain fraudulent data, and can convert the necessary data to data with pre-established, safe, and internal format. Data with an external format the ~~sever~~ server 3 received through the network 1 (shown in Fig. 1) can be written into the received data storage means 6. The host computer 10 does not directly access this received data storage means 6. As a result, the host computer 10 can be prevented from obtaining fraudulent data from the network 1.

Please replace the paragraph at page 18, lines 5-19, with the following rewritten paragraph:

In the system in Fig. 4, the host computer 10 has the ~~received~~ transmit data storage means 12, the ~~received~~ transmit data format conversion means 13 and the transmit process data storage means 14. The ~~remained~~ remainder of the system is

similar to the system shown in Fig. 1. The host computer 10 is adapted to execute ordering administration and the like in the use of the database storage section 9. The ~~received~~ transmit process data storage means 14 can be a storage device to store data with the internal format which the host computer generates and sends over the network. The transmit data format conversion means 13 is adapted to convert data with the internal format stored in the transmit process data storage means 14 to data with an external format and to create the data stored in the transmit data storage means 12. This, as well as the example in Fig. 1, can comprise a computer program and the like. The server 3 is adapted to send data with an external format stored in the transmit data storage means 12 to the network. The content and format of data with an external format and internal format is generally the same as the example in Fig. 1.

Please replace the paragraph at page 18, line 20 to page 19, line 2, with the following rewritten paragraph:

In this system, if the host computer 10 has data to be sent through the network, the host computer can ~~covert~~ convert this to the data with the internal format with selective timing and can store the data in the ~~received~~ transmit process data storage means 14. The transmit data format conversion means 13 can be, for instance, activated in each case by the host computer, and can read out data with the internal format from the transmit process data storage means 14 and convert data with the internal format to data with an external format. The transmit data format conversion means 13 can then write data with an external format to the transmit data storage means 12. This action is different from the case of data received in Fig. 1. As the transmit data format conversion means 13 can acquire information on emergency of sending data from the host computer, the timing of sending data should be classified.

Please replace the paragraph at page 19, lines 10-18, with the following rewritten paragraph:

Furthermore, the transmit process data storage means 14 can preferably allow data with the internal format to be read out by the transmit data format conversion means 13, and can prevent data from being written by the transmit data format conversion means 13. The transmit data storage means 12 can preferably allow data with an external format the server sends to be written by the transmit data format conversion means 13, and can prevent data from being read out by the ~~received~~ transmit data format conversion means 13. As stated above, it is feasible to prevent hackers from stealing data by arranging several barriers with one way flow to the network.

Please replace the paragraph at page 19, lines 19-30, with the following rewritten paragraph:

The conversion process of data with the internal format to data with an external format by the ~~received~~ transmit data format conversion means 13 can be executed with independent timing from the storage process of data with the internal format to the transmit process data storage means 14 by the host computer 10. The system combining the system to receive data indicated in Fig. 1 and the system to send data indicated in Fig. 4 can present extremely high security as far as received and transmitted data is concerned. It is preferable that the conversion process by the received data format conversion means 7 shown in Fig. 4, the additional storage process of data with the internal format to the database of the host computer 10 side, the storage process of data to the ~~received~~ transmit process data storage means 14 by the host computer 10 and the conversion process by the ~~received~~ transmit data format conversion means 13 are each preferably executed with independent timing.

Please replace the paragraph at page 21, line 23 to page 22, line 5, with the following rewritten paragraph:

In other words, the mail client 31 can send data with the mail format to the mail receiving section 41, but does not have a mail receiving function. The mail server 32 receives mails from the mail sending section 42 but does not have a mail sending function. A dedicated communication line for transferring should be used to make connection between the server 3 and the mail transfer section 40. As such, the server 3 and the mail transfer section 40 can be constituted separately from a hardware point of view. To enhance the security even more, the communication line is preferably one which does not have a invading route of other data. As only data with a mail format, not data with ~~the other~~ another format is transferred, ~~and~~ fraudulent commands or data can not be taken to the host computer and the like. Therefore, to provide enhanced reliability, this communication line is preferably a one-way data transfer path. This can provide the improved system security.